ABSTRACT OF THE DISCLOSURE

A complete, scalable approach for establishing secure multicast communication among multiple multicast proxy service nodes of domains of a replicated directory service that spans a wide area network. In one feature, the multicast proxy service nodes are arranged in a binary tree architecture at the LAN level, thereby eliminating the single point of failure of traditional approaches. In another feature, scalability is achieved by using an operationally optimized broadcast version of Diffie-Hellman key exchange that reduces the number of rounds of messages needed to exchange keys. Alternatively, scalability is achieved using a new method for coming to a shared secret in nodes of a broadcast group. Using either feature, a secured communication channel is provided among a plurality of distributed multicast proxy service nodes at the LAN level. According to another feature, a tree approach is used to spread the multicast proxy service nodes at the WAN level, further improving scalability. A directory replication approach is used to distribute private keys of the multicast proxy service nodes, thereby achieving near perfect forward and backward security among nodes at the WAN level. The binary tree architecture is exploited to reduce the overhead involved in calculating new keys by having a local multicast key distribution node serve as a local group member and also manage joining new nodes and determining the new keys.